BESAFE 51

Bulletin d'information sur la sécurité et la prévention locale
JUILLET 2019

ibz

P7088831 | Bureau de dépot Anvers X
Paraît 5x par an

© PHOTO CITYMESH

TECHNOLOGIE

Interview avec Claudia De Maesschalck, Chief Disruption Officer

"Pour lutter contre les réseaux malintentionnés, nous avons besoin de réseaux bienveillants"

Dans certaines grandes organisations, l'innovation est dirigée par un Chief Disruption Officer. Le SPF Intérieur en a récemment également désigné un. La tâche du CDO Claudia De Maesschalck se concentre sur les réseaux malintentionnés utilisant les nouvelles technologies.

Vous avez été désignée comme première Chief Disruption Officer pour les autorités compétentes pour la Sécurité, et en premier lieu pour le SPF Intérieur. Vous êtes installée au sein de la DG Sécurité & Prévention. Qu'implique cette fonction précisément ?

Claudia De Maesschalck : « Tout d'abord, j'aimerais esquisser le contexte : il y a quelques années, IBZ était présent à un congrès sur l'évolution exponentielle des nouvelles technologies et la manière dont elles peuvent attaquer les écosystèmes bienveillants si nous ne nous préparons pas de manière proactive. Songez au retail et au e-commerce ou à l'ubérisation des biens et services à domicile. Mais c'est principalement dans l'écosystème de la sécurité que nous ne pouvons pas nous reposer sur nos lauriers. Les réseaux malintentionnés se servent abondamment des nouvelles technologies et n'ont, par définition, pas les freins qui constituent l'essence d'un réseau bienveillant, à savoir : des limites éthiques, réglementaires et légistiques. Et on peut y ajouter aussi des limites budgétaires. En d'autres termes, nous devons oser agir de manière disruptive afin de saper leur « business model » qui est fortement axé sur les technologies. Il y a quelques années, les esprits n'étaient peut-être pas encore prêts. A présent, ils le sont. »

> « Dans l'écosystème de la sécurité, nous ne pouvons pas nous reposer sur nos lauriers. »

Vous dites que les esprits sont désormais prêts. Pouvez-vous expliquer ce point ?

Claudia De Maesschalck : « Peter Hinssen, l'un des gourous « tech » qui a inspiré Niveau S l'affirme clairement : « *it takes a network to beat a network* », et également que la préparation pour « *The day after tomorrow* » doit commencer dès maintenant. Alors que nous sommes malgré tout toujours occupés à – vous m'excuserez l'expression – ranger le désordre de ce qui s'est passé hier. Ce point de vue a permis d'organiser le Congrès Niveau S du 19-20 décembre de l'année passée. Ce Congrès a été organisé par IBZ et VIAS en étroite collaboration avec le Cabinet ministériel, et a réuni de manière très transparente les services de sécurité, les acteurs privés, les centres de connaissances et les citoyens. L'objectif était de réfléchir de manière conjointe sur la manière de nous préparer au « jour après demain », en guise de réseau bienveillant, cohérent et solide afin de lutter contre l'effritement du tissu social par les réseaux malintentionnés et leur modèle de sapement. Le Congrès a abouti à une série de conclusions et de recommandations, et c'est à présent ma mission de les traduire en une nouvelle politique durable. »

NUMERO THÉMATIQUE

Les nouvelles technologies jouent un rôle de plus en plus important dans la sécurité et la prévention. Besafe apporte un aperçu.

▶ *suite de la page 1*

Pourquoi vous a-t-on demandé à vous, personne externe, d'assurer cette fonction étant donné que vous relevez du SPF Affaires étrangères ?

Claudia De Maesschalck : « La transposition politique de Niveau S est, par définition, transversale et dépasse les cloisonnements. Dans ce sens, c'est un avantage que je ne vienne pas moi-même d'un silo de sécurité, mais que j'arrive avec de l'expérience dans les matières liées à la sécurité. Quand je suis devenue Présidente de l'Autorité nationale de Sécurité, durant la période des attentats, j'ai travaillé avec les Services de sécurité. Par ailleurs, je me suis spécialisée, durant ma carrière diplomatique de plus de 25 ans, dans la diplomatie scientifique et technologique. C'est ce qui fait que j'ai également, outre les acteurs publics, un réseau élargi au sein des centres de connaissances et de l'industrie technologique. Par ailleurs, les ambassadeurs ont de toute façon un réseau élargi et divers. »

Encore une question sur la fonction : pourquoi précisément Chief Disruption Officer, et non Chief Innovation Officer ?

Claudia De Maesschalck : « Parce que les initiatives qui dépassent les cloisonnements requièrent bien plus qu'une approche incrémentale. L'innovation est une préoccupation qui va de soi. Les technologies que nous souhaitons explorer ne sont peut-être pas disruptives en soi, mais la manière dont elles seront englobées et intégrées au sein des applications de sécurité par les autorités le sont. Les solutions seront disruptives, les manières dont elles seront explorées et utilisées également. Cela vaut aussi pour l'état d'esprit qui est nécessaire à cet effet. La disruption est ici autant indiquée, si pas indispensable. Je ne souhaite en effet pas attendre le plus lent ou le plus hésitant, bien au contraire : nous allons travailler avec une avant-garde d'« early adopters », de telle manière que les autres peuvent encore y adhérer, mais sans attendre le peloton. C'est également disruptif. »

> « Les réseaux malintentionnés se servent abondamment des nouvelles technologies et n'ont, par définition, pas les freins qui constituent l'essence d'un réseau bienveillant, à savoir : des limites éthiques, réglementaires et légistiques. »

Quels sont, concrètement, les chantiers que vous démarrez actuellement ?

Claudia De Maesschalck : « Il y a plusieurs chantiers ; tous ont une propre finalité mais ils se renforcent parallèlement. Trois d'entre eux ressortent particulièrement : en premier lieu, la création d'un cadre juridique durable au sein duquel les quatre quadrants – autorités, secteur privé, centres de connaissances et citoyens- au sein de la sphère de sécurité peuvent se rencontrer de manière structurelle : afin de progresser, réunir l'offre et la demande as is et to be. Ainsi, nous pourrons non seulement collaborer de manière ciblée et par projets, mais nous donnerons également une forme juridique au réseau bienveillant. Tous les services publics peuvent non seulement y rassembler leur inventaire de ce qui existe déjà, mais également établir la cartographie des besoins. Cela doit permettre l'optimalisation entre ce qui est déjà et ce qui doit être entre tous les demandeurs et les offrants. Sans chevauchement, fragmentation ou programmation contradictoire.

Un deuxième chantier concerne davantage le "faire". Il est nécessaire de lutter contre le morcellement de la récolte et du stockage d'informations. Au sein des autorités – songez aux recommandations POC, – mais également avec le "monde extérieur". Les autorités ne souhaitent pas avoir accès aux données privées, bien au contraire : il appartient à nos missions de les protéger. D'autre part, il y a encore trop souvent une distinction entre l'intégrité de l'identité physique et celle de l'identité numérique. En ce qui concerne ce dernier point, il existe de nouvelles responsabilités pour tous les "titulaires" de données et les aperçus de données : autorités, secteur privé et citoyens. Les autorités peuvent bien avoir le monopole de la violence, mais elles ont perdu depuis longtemps celui de l'information. Ce n'est pas en soi une catastrophe ; les autorités doivent pouvoir veiller à ce que l'intégrité de l'identité numérique, ou plutôt les identités, car celles-ci sont morcelées entre diverses plateformes, soit assurée. C'est dans l'intérêt des autorités, des acteurs privés et, encore davantage des citoyens. Il nous appartient de trouver, au moyen d'une gestion de données adulte, un équilibre adéquat entre une imagerie efficace et la proportionnalité. En ce sens, j'attends avec impatience de découvrir la synthèse des différentes initiatives démarrées ou presque entamées à différents niveaux de pouvoir et les initiatives que la prochaine Commission européenne démarrera. A cet égard, cela sera non seulement "bâtir", mais également intégrer et revaloriser. Je souhaite dans cette optique jouer un rôle de charnière entre différents niveaux de pouvoir et les technologies, et entre les théories et les concepts scientifiques. »

Et le troisième chantier ?

Claudia De Maesschalck : « C'est en soi un chantier transversal : dans tout ce que nous faisons, à savoir fixer des priorités, stimuler de nouvelles technologies ou réunir des suspects inhabituels, tout doit être analysé. Non seulement en termes de faisabilité et de coût, mais également en termes d'opportunité et d'acceptabilité. C'est pourquoi je plaide vigoureusement en faveur de la création d'un Conseil pluridisciplinaire qui offre la possibilité de nous accompagner dans le cadre réglementaire et législatif. Ici aussi, la proportionnalité est un fil rouge. Si les autorités veulent rester pertinentes, nous ne pouvons pas nous transformer en un « oncle » qui gâche tout. Nous devons pouvoir être un chouette « oncle » qui participe à la fête et qui se montre inspirant et reflète la confiance. Ainsi, la fête continue à attirer un public plaisant sans que les choses ne dégénèrent. »

Est-ce que cette nouvelle technologie ne risque pas de devenir le scénario catastrophe de Big Brother ou de Minority Report ?

Claudia De Maesschalck : « C'est pourquoi nous avons précisément besoin d'un Conseil éthique. Cependant, ne pas englober la nouvelle technologie et ses possibilités est en soi encore peu éthique : cela laisse le champ libre aux réseaux malintentionnés actionnés par la technologie, et affaiblit ainsi les autorités dans l'une de ses missions essentielles, à savoir la protection de la sécurité générale au sein des réseaux bienveillants.

Non seulement, nous devons changer notre fusil d'épaule, mais nous devons également le remplacer : ce point de vue est partagé par tous les chefs. Que ce soit des services de sécurité ou d'autres partenaires privés qui souhaitent tous contribuer à un réseau bien intentionné actif et large. Afin de réaliser ce shift de paradigme, il est par contre essentiel de commencer à petite échelle. Avec des fruits faciles à cueillir. Avec des casus bien réfléchis qui peuvent faire tache d'huile et qui, grâce à leur utilité prouvée, peuvent inspirer et en stimuler d'autres. C'est pourquoi je me réjouis qu'au sein de tous les services, un SPOC (single point of contact) ait été désigné qui est proche des chefs, et qui connaît extrêmement bien le terrain afin de pouvoir mettre en place des champs d'expérimentation bien focalisés avec le soutien de leur hiérarchie. »

© PHOTO CLAUDIA DE MAESSCHALCK

CDO Claudia De Maesschalck : « Non seulement, nous devons changer notre fusil d'épaule, mais nous devons également le remplacer »

The Internet of Things : utile pour la prévention des cambriolages, mais aussi pour les cambrioleurs

Les ordinateurs, smartphones et/ou tablettes ne sont pas les seuls appareils à pouvoir être connectés à Internet. D'autres appareils tels que les réfrigérateurs, les machines à laver et les thermostats peuvent également être connectés.

Lentement mais sûrement, l'Internet of Things (IoT) transformera le monde qui nous entoure. Selon les prévisions, d'ici 2020, plus de 20 milliards d'objets seront connectés à Internet, entre eux et certainement avec des applications. L'IoT a pour but de nous simplifier la vie. Grâce à la connexion à Internet, de bêtes objets gagneront souvent en utilité et leur champ d'utilisation sera peut-être plus vaste.
L'exemple le plus connu d'objet connecté est le frigo intelligent : cet appareil détecte quand la date de péremption de vos produits est dépassée, il réduit la température en cas de fortes chaleurs et gère l'approvisionnement. Tout cela grâce à des détecteurs dans le frigo, à une connexion Internet, et à un système intelligent qui enregistre vos consommations.
D'autres objets connectés permettent une meilleure protection de votre habitation. Il suffit de penser notamment aux caméras de surveillance et aux serrures intelligentes que vous pouvez contrôler à partir d'une application installée sur votre smartphone. Vous pouvez ainsi encore mieux protéger votre habitation. Oui, mais ... L'IoT comporte aussi certains risques.
L'internet reste un environnement méconnu qui se développe très rapidement, ce qui peut entraîner un risque de protection moins efficace et de piratage de votre réseau wifi. Chaque connexion de vos objets intelligents à Internet est une cible potentielle pour les criminels qui veulent en prendre le contrôle, par exemple pour forcer et ouvrir votre serrure intelligente et accéder ainsi à votre habitation.
Pour éviter ce genre d'incidents, une sécurisation efficace de votre réseau wifi et de vos appareils IoT peut déjà s'avérer très utile. Voici quelques conseils :

- prévoyez plusieurs niveaux de sécurité pour chaque appareil connecté : par exemple, vous pouvez combiner la serrure intelligente de votre porte de devant ou de derrière à une application mobile nécessitant un code d'accès ou un empreinte digitale ;
- sécurisez toujours votre réseau sans fil au moyen d'un mot de passe fort.

Ainsi, votre habitation avec des objets connectés reste protégée de manière optimale. Vous pouvez également faire appel à un conseiller en prévention vol qui vous donnera des conseils sur mesure et sans engagement.

Liens utiles

- www.besafe.be/fr/actualités/soyez-malin-et-securisez-egalement-vos-appareils-intelligents
- www.safeonweb.be/fr/utilisez-des-mots-de-passe-surs

De la sonnette intelligente au thermostat et au vélo

L'Internet of Things a déjà de nombreuses applications qui peuvent aider à lutter contre le vol.
Prenons l'exemple de la sonnette intelligente. Celle-ci vous permet, grâce à votre smartphone, de vérifier qui est devant votre porte. Vous pouvez communiquer avec le visiteur et vous donnez ainsi l'illusion que vous êtes à la maison. Si toutefois vous êtes méfiant, vous pouvez, à distance, mettre de la musique dans votre habitation. Cela donnera encore plus l'impression que vous êtes vraiment chez vous. Une évolution dans la prévention des vols !
En outre, il ya également le thermostat qui peut être commandé à distance aux heures adéquates, ainsi que les lampes intelligentes, tous deux des éléments de l'Internet of Things. L'automatisation de la connexion avec les lampes dans la maison peut également simuler une présence même s'il n'y a personne dans l'habitation. C'est un instrument de lutte contre les vols dans les habitations. Il en est de même pour les volets qui peuvent être commandés à distance, même si vous êtes en vacances.
Enfin, il y a le vélo intelligent développé aux Pays-Bas et équipé d'un capteur spécial. Un vendeur de vélos peut fixer ce capteur sur n'importe quel vélo avec de la colle industrielle. Le capteur est de base toujours éteint, d'où sa très faible consommation d'énergie et le risque peu élevé de tomber en panne. Si un vélo est volé, le propriétaire légitime du vélo peut activer le capteur grâce à une application pour smartphones. Une fois activé, le capteur du vélo envoie ses données de localisation à une équipe de recherche qui peut ainsi voir où se trouve le vélo volé et peut immédiatement agir pour retrouver celui-ci.

Le smartphone, point de départ de la commande à distance du thermostat, de la sonnette, des volets, et de l'éclairage.

© PHOTOSHUTTERSTOCK

Des caméras de surveillance de plus en plus efficientes

La caméra de surveillance est aujourd'hui devenue l'outil par excellence pour sécuriser tant la voie publique que les bâtiments ou espaces fermés, qu'ils soient publics, privés ou complètement privatifs.

Avoir des images, pouvoir les consulter sur place ou à distance, pour les visionner en temps réel ou a posteriori, apporte un élément rassurant, un sentiment que s'il se passe quelque chose, on en connaîtra les causes et on saura réagir de manière adéquate.
Mais si lorsque les premiers systèmes de CCTV ont commencé à être utilisés, il s'agissait uniquement de collecte et d'enregistrement d'images, la technologie permet aujourd'hui d'aller bien plus loin. Qu'il s'agisse de caméras dotées d'un détecteur de sons, de chaleur, de mouvements, de caméras de reconnaissance automatique de plaques d'immatriculation, ou de caméras de reconnaissance faciale, les systèmes de surveillance sont de plus en plus équipés d'une solution d'analyse d'image, voire dotés d'AI, permettant de donner une alerte quand un événement se produit, de filtrer les images, de les trier, de les structurer. Dans tous les cas, cette intelligence permet d'augmenter l'efficience des caméras de surveillance installées, et en cas de visionnage en temps réel des images, elle constitue également une aide pour les opérateurs. Par ailleurs, la qualité des images a aussi sensiblement augmenté, les capacités de stockage également, ce qui permet d'affirmer que les images deviennent un élément incontournable de preuve.
A ce propos, la nouvelle application mise en ligne en 2018 pour les déclarations de caméras de surveillance, permet aux services de police de savoir où sont installées des caméras de surveillance et qui contacter pour pouvoir demander l'accès aux images, dans le cadre de leurs missions de police. Le premier réflexe lorsque des faits se produisent est, en effet, de se poser la question de la présence de caméras et de l'existence d'images.
Bien entendu, quelle que soit la technologie concernée, elle doit être utilisée en tenant compte de la législation en vigueur, en matière de protection des données à caractère personnel et des contraintes de la loi caméras[1], mais il est clair que l'avenir ne s'envisage pas sans caméras de surveillance, qui plus est sans caméras de surveillance intelligentes.

Lien utile

- www.besafe.be/fr/themes-de-securite/camera/loi-cameras

1 Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, telle qu'elle a été sensiblement modifiée par la loi du 21 mars 2018.

Caméras avec reconnaissance faciale : il y a toujours des obstacles pour la vie privée

Il y a huit ans, la zone de police RIHO a testé quatre caméras numériques avec reconnaissance faciale.
À l'époque, elles ont été utilisées lors des enregistrements de l'émission de télévision « Villa Vanthilt » qui attirait tous les jours environ 800 personnes sur la grand-place. Ce chiffre avait également été calculé par les caméras intelligentes.
Les images des caméras avaient été envoyées au dispatching via le réseau 3G de Belgacom. Roulers avait alors été la première ville à expérimenter cette technologie. « Il s'agissait d'un projet unique que nous avons testé en collaboration avec Belgacom, qui prenait également une partie des frais en charge », explique Tineke Verduyn de la ZP RIHO. « En guise de test, nous avons alors lié les images à une banque de données contenant des photos. Plusieurs personnes y ont alors apporté leur collaboration. Afin de poursuivre le projet, nous aurions dû disposer d'une plus grande banque de données mais des obstacles juridiques se sont élevés. De plus, la technologie n'était pas totalement au point à ce moment-là. La situation s'est aujourd'hui indéniablement améliorée et les réseaux sont beaucoup plus rapides. Entre-temps, nous avons fait l'acquisition de la nouvelle technologie Video Synopsis qui rend nos 128 caméras « intelligentes ». Le système nous permet non seulement de rechercher de manière ciblée des personnes mais aussi des véhicules, tant en temps réel que sur des images enregistrées. »

Courtrai utilise également cette technologie pour tester les limites des possibilités. Ce logiciel enregistre tous les objets présents sur l'image des caméras et les filtre sur la base de caractéristiques comme le genre ou les vêtements des personnes. Le logiciel peut également reconnaître des visages, mais étant donné qu'il subsiste des limitations légales à ce sujet, cette fonctionnalité n'est pas encore utilisée à Courtrai.

Les caméras intelligentes peuvent filtrer des personnes dans une foule sur la base de caractéristiques comme le genre ou les vêtements.

© PHOTO BELGAIMAGE

Drone : d'objet volant non identifié (OVNI) à véhicule aérien sans pilote (VASP)

Vous avez probablement déjà dû voir un drone ou VASP voler. Nous les connaissons surtout comme jouets technologiques pour adolescents, ou plus récemment, comme moyen de gardiennage pour la police. Mais les drones sont devenus entre-temps bien plus que cela.

Ils peuvent être équipés d'une caméra visuelle ordinaire comme vous le savez certainement, mais également de caméras thermiques, de senseurs, d'un système de navigation pour pouvoir voler de manière autonome, mais aussi d'un numéro de plaque électronique pour les identifier. Ils peuvent ainsi être équipés de AI dans le cadre d'opérations anti-drones.

Il existe d'innombrables applications qui découlent de la technologie de drones :

- gardiennage d'événements publics et de zones industrielles ;
- entretien d'entreprises et de turbines à vent (offshore), où les drones vérifient les installations en les survolant en filmant alors qu'un technicien à terre reçoit et analyse ces images ;
- Google et Amazone développent des services de livraison avec des drones autonomes ;
- lorsqu'un incendie éclate à Anvers, un drone autonome vole vers le foyer d'incendie. Ce drone filme l'incendie et envoie les images en temps réel vers le véhicule des services d'incendie avant qu'il n'arrive. Et des drones peuvent également détecter des incendies de forêts dans les coins reculés.

Cependant, quelques risques non négligeables y sont associés. Ainsi, le risque de panne est beaucoup plus élevé que pour un avion. La technologie est par définition neutre et peut être utilisée tant à des fins honnêtes que malhonnêtes. C'est pourquoi nous avons comme rôle en tant qu'autorités d'influer sur les nouvelles évolutions et nous veillons à lutter contre l'utilisation de nouvelles technologies à des fins malintentionnées.

Il est de ce fait important de savoir que les drones sont soumis à de nombreuses réglementations, en fonction de leur application, dont en premier lieu l'AR drones. Pour les drones de gardiennage qui sont équipés d'une caméra (caméras mobiles), la Loi caméras et la Loi RGPD sont applicables pour le traitement des données à caractère personnel. La Loi sur la fonction de police régit enfin l'utilisation des drones par la police.

Les drones ne seront ainsi plus à vos yeux des objets volants non identifiés.

Lien utile

- www.besafe.be/fr/themes-de-securite/camera/utilisation-de-cameras-par-les-services-de-police/d-quelles-cameras-quand

La ZP CARMA utilise un robot subaquatique pour effectuer des recherches

La zone de police CARMA (As, Bocholt, Bree, Genk, Houthalen-Helchteren, Kinrooi, Oudsbergen, Zutendaal) a mis en service un ROV ou « remotely operated underwater verhicle » en 2016. Le ROV est doté d'un éclairage et de caméras et il peut être utilisé pour effectuer des recherches sous l'eau de manière ciblée. La police peut ainsi agir plus vite en cas de disparitions ou dans le cadre de dossiers judiciaires. La zone a développé elle-même le robot subaquatique en collaboration avec quelques experts.

Le ROV est un petit appareil maniable, qui peut être actionné à l'aide d'une commande à distance depuis le rivage ou depuis un bateau. Les images qui sont réalisées par le ROV peuvent être suivies en direct sur un moniteur. L'appareil ne peut pas manipuler d'objets ou les ramener à la surface. La police continue donc à faire appel à une équipe de plongeurs des pompiers ou de la Protection civile dès que quelque chose de suspect est découvert, ou s'il s'agit de recherches à une profondeur trop importante ou sur une trop grande surface.

« Nous utilisons l'appareil pour des missions ciblées », indique la porte-parole Marleen Smeyers. « Étant donné que nous pouvons le déployer rapidement, il peut déjà nous donner une image avant même l'arrivée des services spécialisés sur place. Il présente par ailleurs des avantages par rapport aux plongeurs : il occasionne moins de remous sous l'eau de sorte que la vision des caméras n'est pas dégradée par les turbulences dans l'eau et le sable qui tourbillonne. Comme nous pouvons aussi déployer l'appareil en combinaison avec un bateau, il est possible d'effectuer des recherches sur une zone plus étendue. »

Le robot subaquatique de la ZP CARMA est petit et peut donc être rapidement mis en œuvre.

© PHOTO PZ CARMA

Data insight sharing : une nouvelle génération de partage de données

Vu que les data ne sont plus le monopole des autorités, il y a de nouvelles responsabilités pour tous les « titulaires » de données et les aperçus de données : autorités, secteur privé et citoyens.

En effet, les autorités de sécurité peuvent bien avoir le monopole de la violence, mais elles ont perdu depuis longtemps celui de l'information. Ce n'est pas en soi une catastrophe, mais les autorités doivent pouvoir veiller à ce que l'intégrité de l'identité numérique, ou plutôt les identités, car celles-ci sont morcelées entre diverses plateformes, soit assurée. C'est dans l'intérêt des autorités, des acteurs privés et, encore, des citoyens le plus.

Une plateforme « nouvelle génération » de partage de données et d'aperçus de données devra voir le jour. Cette nouvelle architecture sera sans doute hybride, avec une colonne vertébrale, mais aussi avec des éléments de technologie blockchain de la 3e ou 4e génération.
Dans tout cela, il nous appartient de trouver, au moyen d'une gestion de données adulte, un équilibre adéquat entre une imagerie efficace et la proportionnalité.

Déjà des différentes initiatives ont démarrées ou sont presque entamées à différents niveaux de pouvoir, y compris par la Commission européenne qui se prépare à une nouvelle vision de partage de données basée sur le concept de « self souvereign identity », qui donne un nouveau pouvoir au citoyen sur la manière de partager et d'utiliser ses propres informations digitales.

La ZP Brasschaat enregistre des infractions routières avec un smartphone

Depuis 2016, les collaborateurs du service circulation de la zone de police Brasschaat travaillent avec des « handhelds » (sortes de smartphones) qui leur permettent de constater les infractions routières de manière simple et rapide. Toutes les données sont immédiatement enregistrées et traitées en rue via un logiciel adapté. « Les agents prennent une photo de l'infraction, enregistrent la plaque d'immatriculation du véhicule et complètent les données correspondantes. Au commissariat, les données sont ensuite automatiquement téléchargées sur le réseau de la police. Tout se fait automatiquement. Grâce aux smartphones, les agents et inspecteurs peuvent être plus présents en rue », précise l'inspecteur principal Werner Hoogsteyns, responsable de la circulation de la ZP Brasschaat.
Les smartphones Android sont développés par la société Tradelec, qui est basée à Genk, pour répondre aux besoins de la police et sur la base d'observations sur le terrain. Le code-barres d'une carte d'identité peut être scanné et ajouté pour assurer un traitement correct et rapide des identités. Les appareils sont renforcés (« ruggedized ») et ont un haut degré d'étanchéité.
« Nous utilisons actuellement 4 appareils », ajoute Werner Hoogsteyns, « mais nous allons prochainement en ajouter deux en raison du succès remporté ».

© PHOTO PZ BRASSCHAAT

Werner Hoogsteyns: « Les handhelds s'inscrivent dans le plan politique de la direction visant à avoir plus de bleu en rue. La police doit pouvoir se concentrer sur ses missions de base et un allégement de la charge de travail administratif doit se poursuivre en simplifiant les processus opérationnels et en les numérisant. »

Lancement de l'app policière FOCUS@GPI

Depuis février de cette année, les policiers peuvent accéder rapidement et facilement au Casier judiciaire, au Registre national, et à la banque de données des plaques d'immatriculation. Cela se fait via l'app policière Focus@GPI. Cette même app leur permet également de dresser procès-verbal ou de consulter d'autres informations utiles. Les collaborateurs du dispatching sont partiellement soulagés d'une partie de la charge de travail étant donné que les données à caractère personnel peuvent être demandées directement via l'app.
En première instance, l'app a été mise à la disposition des quatre zones de police flamandes Druivenstreek, Voorkempen, Westkust et Antwerpen, de la police fédérale de la route d'Anvers, des deux zones bruxelloises Polbruno et Marlow, ainsi que des trois zones wallonnes Namur, Mons-Quévy et Weser-Göhl. D'ici l'année prochaine, le système sera étendu aux autres zones de police et unités de la police fédérale de la route.
Grâce à l'app, les policiers ont accès aux banques de données via leur téléphone, ce qui se fait bien sûr suivant des règles bien définies. Les banques de données ne peuvent être consultées que si cela cadre avec la fonction ou le rôle opérationnel du policier concerné. Les droits d'utilisation des applications mobiles sont également attribués de manière personnalisée et toutes les recherches effectuées sont enregistrées. Les unités choisissent elles-mêmes dans quelle fonctionnalité de base de la police l'app Focus@GPI est utilisée.

La technologie RFID aide à tracer des personnes et des marchandises

La technologie RFID (Radio Frequency IDentification) est utilisée pour identifier et localiser à distance des personnes ou des objets. Cette technologie fonctionne au moyen de signaux radio.

Le système utilise des étiquettes ou des tags qui se trouvent sur les personnes ou les objets. Ces tags sont munis d'une puce électronique et d'une antenne. Ils émettent des signaux sur une certaine fréquence radio qui sont alors captés par un lecteur. Chaque objet contenant un tag RFID possède une identité ou un numéro unique qui peut être ainsi transmis à ce lecteur.

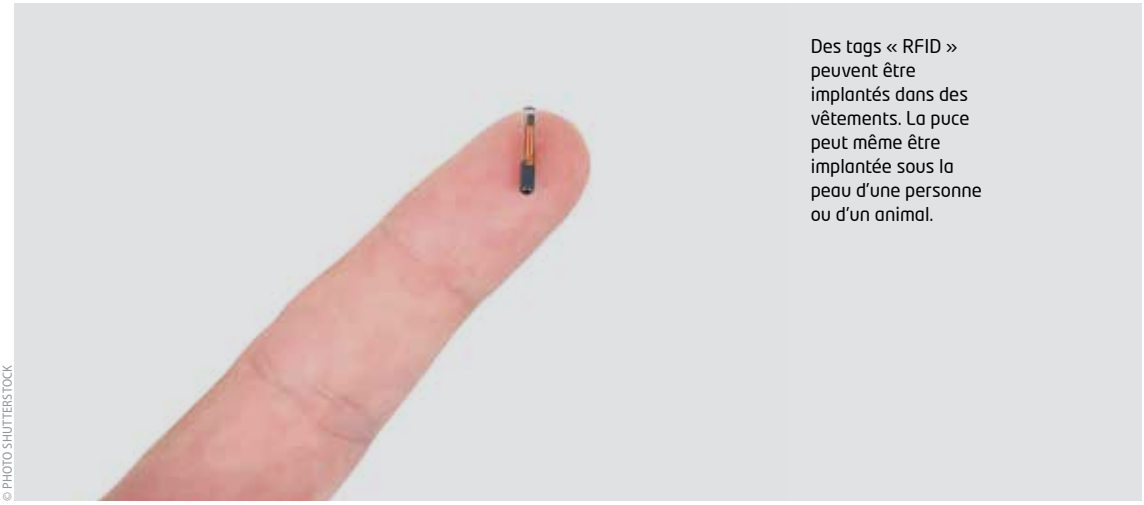
Grâce à leur puce électronique, les tags offrent plus de possibilités que des codes-barres classiques. Ils ne sont lisibles uniquement que s'ils se trouvent dans le rayon optique du scanner.

Les tags peuvent être passifs et prendre la forme d'une étiquette à coller, par exemple sur un colis, voire d'un implant pouvant, en théorie, être placé sous la peau d'un organisme vivant. Quant aux tags actifs, ils décuplent les effets des tags passifs et ont une source autonome de tension.

La technologie RFID est principalement utilisée dans le secteur de la distribution pour faciliter l'identification, l'inventaire et la localisation des produits. On trouve également cette technologie, par exemple, dans les titres de transport, les badges d'accès, et dans nos passeports. Etant donné que cette technologie peut aussi être associée à des individus, la protection de la vie privée représente un aspect essentiel. Par ailleurs, cette technologie peut parfaitement être implantée dans des vêtements, comme des uniformes. C'est déjà le cas dans les blanchisseries industrielles, ou sur des bateaux de croisière et dans d'autres environnements où le personnel porte un uniforme. Les vêtements peuvent être ainsi localisés en cas de vol ou d'utilisation non autorisée.

Ces tags peuvent cependant être assez facilement découpés ou retirés après avoir été implantés dans des vêtements. Voilà pourquoi des recherches ont été menées sur des textiles entièrement constitués de la technologie RFID. En d'autres termes : le textile à proprement parler devient un « RFID tag portable ».

« Cette technologie peut être extrêmement appropriée pour sécuriser des vêtements, y compris des uniformes. »



© PHOTO SHUTTERSTOCK

Des tags « RFID » peuvent être implantés dans des vêtements. La puce peut même être implantée sous la peau d'une personne ou d'un animal.

« Et maintenant ? »

Comme il ressort des encadrés ci-dessus, chaque technologie entraîne à la fois des avantages et des inconvénients. Par définition, ceux-ci sont plus difficiles à évaluer dans le cas de nouvelles technologies disruptives : ces dernières vont-elles tenir leurs promesses ? Et à quels effets secondaires, positifs et négatifs, peut-on s'attendre ? C'est surtout ce dernier point qui rend l'exercice sensible, car tous les effets secondaires néfastes et leur impact ne sont probablement pas possibles à évaluer pour le moment. Nous ne pouvons nous laisser prendre en voyant les nouvelles technologies comme un but en soi. Elles doivent rester des moyens, dans notre cas, pour atteindre une finalité déterminée au sein des missions de sécurité distinctes.

« Nous avons besoin d'un Conseil éthique, certes, mais nous devons continuer à faire, pour nous-même, la pondération entre les coûts et les profits, à savoir les coûts et profits dans le sens littéral du terme, tout comme de nature morale et déontologique. »

Lors de cet exercice qui nous concerne tous, c'est donc un exercice d'équilibre entre le souhaitable, le réalisable et le permissible. A cet effet, nous avons besoin d'un Conseil éthique, certes, mais nous devons continuer à faire, pour nous-même, la pondération entre les coûts et les profits, à savoir les coûts et profits dans le sens littéral du terme, tout comme de nature morale et déontologique. Et dans tout cela, cet exercice d'équilibre consiste à s'assurer que notre service public continue à jouer un rôle stimulant et pertinent qui, certes, interdit certaines choses, mais permet également la création d'un climat de recherche et d'investissement approprié, sans perdre de vue les aspects éthiques. Nous nous trouvons en grande partie sur un terrain vague. Cela a également des avantages et des inconvénients. Nous ne rencontrons pas « les freins de l'avancée » mais nous ne disposons pas encore d'une expérience élargie et suffisante sur laquelle nous pouvons nous baser en cas de doute. C'est pourquoi il est recommandé de commencer à petite échelle, avec des champs d'expérimentation clairement définis.

A cet égard, la question devra également être posée de savoir s'il ne faut pas prévoir un régime juridique spécial dans le cadre de certains champs d'expérimentation et projets, où certaines exceptions clairement définies et proportionnelles au regard de la finalité, peuvent être tolérées et pour lesquelles le contrôle de celles-ci est adéquat et suffisant. Il s'agit d'une question ouverte mais nous ne pouvons pas l'éluder, tout comme d'autres « questions tabous » qui pourraient éteindre le débat avant de l'avoir démarré.
Et ce débat, nous voulons l'entamer avec nos partenaires. Après ce numéro thématique, la disruption et l'innovation seront des thèmes récurrents, sur base de l'interaction mise en place avec vous dans ce Besafe Magazine n°51.

Avez-vous d'autres idées ou une solution possible pour un problème donné dans le contexte de l'innovation et de la perturbation du secteur public? Envoyez vos suggestions à notre boîte à idées DisGover@ibz.fgov.be

Colofon
Abonnement et adresse rédactionnelle : SPF Intérieur, Direction générale Sécurité et Prevention, Boulevard de Waterloo 76, 1000 Bruxelles, 02 557 33 24 Editeur résponsable : Philip Willekens, directeur général Sécurité et Prevention, Boulevard de Waterloo 76, 1000 Bruxelles
Rédaction et réalisation : Wolters Kluwer Comité de rédaction : Caroline Atas, Patrick Barbé, Bianca Boeckx, Claudia De Maesschalck, Matthias Finet, Johan Geldhof, Thomas Gijs, Mathieu Kasiers, Christian Nicolet, Eric Valerio, Bea Vossen, Gaetan Willems www.besafe.be